UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,382	02/13/2004	Graham A. Wheeler	50037.219US01	9021

27488 7590 10/31/2007

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
MEDE, ESTEVE	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,382	WHEELER, GRAHAM A.	
	Examiner	Art Unit	
	Esteve Mede	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

1. Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

2. The rejection of claims under 35 U.S.C 112 is withdrawn

3. Objection to claim 14 remains applicant failed to make required correction.

Claim Objections

4. Claim 14 is objected to because of the following informalities: in claim 14, line 2 the phrase "a time step" should be --a time stamp--. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 11-14, 16-20 rejected under 35 U.S.C. 102(b) as being anticipated by Perrig et al. ("Efficient Authentication and Signing of Multicast Streams over Lossy Channels", 2000).

Regarding claim 11, Perrig discloses a method for authenticating frame transmission from a server to a client device, comprising. Retrieving a Rivest Shamir Adleman (RSA) signed datum from a frame (page 3 col. 2, lines 27-31; see section 3.1 paragraph 1-2); verifying an RSA signature associated with the RSA signed datum from

the frame is explicitly stated by the prior art as the datum is signed with RSA keys (page 3 col. 2, lines 27-31; page 8 col. 1, lines 1-8); storing a hash key that is associated with the frame when the RSA signature is verified (page 9 col. 1, 1st paragraph); receiving another hash key and an HMAC value from the frame (page 9 col. 1, 4th paragraph; page 9 col. 1, 1st paragraph); verifying the HMAC value with the other hash key (page 9 col. 1, 4th paragraph); discarding the frame when at least on of the other hash key and the HMAC value fail verification is an intrinsic property of the claim invention as the discarding a frame which does not verify is the primary function of applying hash key and the HMAC; And, accepting the frame when the other hash key and the HMAC value are successfully verified (page 8 col. 2, lines 45-55).

Regarding claims 12, Perrig discloses the method further comprising a count associated with the client device; computing a hash key using the count and a secret key that is known by both the server and the client; wherein the count corresponds to at least on of a time stamp in the client device; identifying the frame number associated with the frame (page 2 col. 2, lines 1-7; see section 2.2 on page 3; page 7 col. 1, 3rd paragraph).

Regarding claim 13, Perrig discloses verifying the other hash key comprises; receiving a previously stored hash key (page 2 col. 2, lines 1-7; page 5 col. 2, lines 27-27; page 6 col. 1, 2nd paragraph); retrieving a count in the client device is an intrinsic property of the claimed invention as the messages are received in sequence therefore the receiver must have a count in order to decode the content. Computing an expected

hash key from the previous stored hash key and the count (page 5 col. 1, lines 48-49; page 8 col. 2, lines 51-55).

Regarding claim 14, Perrig discloses wherein the count corresponds to a time stamp in the client device (page 15, col. 1, lines 19-20); identifying the frame number associated with the frame (page 2 col. 2, lines 1-7); and identifying the block number associated with the frame is an intrinsic property of the claimed invention as the messages are received in sequence therefore the receiver must have a count in order to decode the content.

Regarding claim 16, Perrig discloses the method further comprising storing a verified hash key for verification of further transmission frames after the hash key is accepted (page 9 col. 1, 1st paragraph).

Regarding claim 17, Perrig discloses a broadcast communication system for communicating frame transmission from a server to a client device, comprising: a scheduler that is arranged to provide data blocks to the server for transmission in a next frame (page 4 col. 4, lines 13-15); a counter that is arranged to provide a count in the server (page 2 col. 2, lines1-7); a hashing function in the server that is arranged to computer hash keys for the next frame using the count and a secret key (page 2 col. 2, lines 1-7); an HMAC function in the server that is arranged to provide an HMAC value in response to hash keys associated with the next frame (page 9 col. 1, lines 41-43); a broadcast processor in the server that is arranged to receive the hash keys, HMAC values, the data blocks and organize the next frame for transmission (see abstract);

such that the data block and the HMAC value appear before the hash key in the frame transmission (page 2 col. 2, lines 1-7; page 3 col. 3, lines 38-43 page 4 col. 2, lines 38-43).

Regarding claim 18 and 20, Perrig discloses the broadcast communication system of claim 17, further comprising a broadcast receiver in the client device that is arranged to receive a transmitted frame (see abstract); wherein the transmitted from starts with another HMAC value, continues with another signed datum followed by another data block and ends with another hash key (page 9 col. 1); a counter in the client device that is arranged to provide another count intrinsic property of the claimed invention as the contains a count of the chains of packet, therefore the receiver must also contains a count in order to verify received frames; a hashing function in the client device that is arrange to compute additional hash keys for the frame transmission using the other count, the secret key and previously stored hash keys, examiner note that the prior art is using hash chaining (page 2 col. 2, lines 1-7; page 9 col. 1, 1st paragraph); a verification function block in the client device that is arranged to verify the other hash key with the additional hash keys and verify the HMAC value with the other hash key and previous hash keys is an intrinsic property of the claimed invention as the feature are needed by the receiver in order for the receiver to be able to very and authenticate the frames. A means for discarding the frame in the client device when at least one of the other hash key and the HMAC value fail verification (page 3 col. 1, lines 8-10); a means for accepting the frame in the client device when the other hash key and the HMAC value are successfully verified is an intrinsic property of the claimed invention as

the function of the receiver is to authenticate (verify) valid frame that it received, and determined is frames are valid or not.

Regarding claim 19, Perrig discloses the broadcast communication system of claim 18, further comprising: a means for recording the other hash key when the frame is accepted (page 9 col. 1, lines 41-43), wherein the other hash key is utilized for verification of subsequently received transmission frames (page 2 col. 2, lines 1-7).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1-10,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mache (US 2001/0002929 A1) in view of Perrig et al. ("Efficient Authentication and Signing of Multicast Streams over Lossy Channels", 2000).

Regarding claim 1 Mache discloses a method for signing transmission from a broadcast server to a client comprises; obtaining a data block that is scheduled for transmission in a next from (para. 0016, lines 1-2; 0037, lines 1-2); selecting a secret key that is associated with the client device for a number of data blocks (para. 0014, lines 3-6; para. 0017, lines 3-5); computing a set of hash keys using the secret key

(para. 0031, lines 1-4; para. 0036, lines 1-4); selecting a hash key that is associated with the data block (see abstract); computing an HMAC value for the next frame using the selected hash key (para. 0037, lines 6-7); periodically signing and transmitting a datum containing the hash key of an earlier or initial frame with a digital signature key (para. 0037, lines 1-4) .

However Mache does not discloses wherein the next frame includes a number of data blocks; generating a count that is associated with time; wherein the selected hash is a set of hash keys using the secret key and the count; and assembling the next frame such that the data block and the HMAC value appear before the hash key in the frame transmission.

Perrig discloses wherein the next frame includes a number of data blocks (page 2 col. 2, lines 1-7); generating a count that is associated with time (page 7 col. 1, 3rd paragraph); wherein the selected hash is a set of hash keys using the secret key is an intrinsic property of the claimed invention as the prior art discloses a hash chains which include more than one hash keys (page 2 col. 2, lines 1-7); and assembling the next frame such that the data block and the HMAC value appear before the hash key in the frame transmission (page 2 col. 2, lines 1-7; page 3 col. 3, lines 38-43 page 4 col. 2, lines 38-43). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Mache to include the use of hash chains such that one may obtain a set of hash keys to encrypt a number of subsequent transmissions in order to provide adequate security over transmission data.

Regarding claim 2, Perrig discloses wherein the datum corresponds to at lest one of (n, S)} k and (n, b, S) where b corresponds to a preceding frame number from a previous frame transmission (page 2 col. 2, lines 1-7)

Regarding claim 3, Perrig discloses the method comprising, selecting the count such that the count is associated with an index of the data block (page 5 col. 1, lines 33-35).

Regarding claim 4, Perrig discloses the method, comprising selecting the count hash such that the count corresponds to a time stamp associated with an internal clock in the broadcast server (page 5 col. 1, lines 33-51; page 5 col. 2 lines 1-5; see section 2-8 on page 6-7).

Regarding claim 5, Mache discloses the method wherein computing the set of hash keys corresponds to applying a one-way function to the secret key (para. 0023, lines 4-7).

Regarding claim 6, Mache discloses the method of claim 1, wherein computing the HMAC value corresponds to a hashed message authentication code, wherein a value (H.sub.i) associated with the hashed message authentication code is given as H.sub.i=HMAC (F.sub.i, S.sub.i), where F.sub.i corresponds to the data being signed, S.sub.i the key for signing, and i the sequence number associated with the data and key (para. 0009, lines 1-9; para. 0086, lines 1-3; para. 0036, lines 1-4).

Regarding claim 7, Mache discloses the communicating parties share a secret key, which can securely exchange periodically (para. 0037, lines 1-3).

Regarding claim 8, Perrig discloses the method of claim 1, wherein periodically signing the datum comprises signing the datum every frame (page 10 col. 1, lines 11-13; page 1 col. 2, lines 23-26).

Regarding claims 9, Perrig discloses the method comprising, incrementing the count before retrieving a data block that is scheduled for transmission in the next frame (page 2 col. 2, lines 1-7).

Regarding claim 10, Perrig discloses the method of claim 9, wherein incrementing the count corresponds to a least one of: incrementing a time stamp in the broadcast server, incrementing the frame number associated with the next frame that is scheduled for transmission (page 2 col. 2, lines 1-7; see section 2.2 on page 3).

9. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perrig et al. ("Efficient Authentication and Signing of Multicast Streams over Lossy Channels", 2000) in view of Carro (US 2004/0054906 A1).

Regarding claim 15, Perrig discloses *i* sequence number associated with the data and key (page 2 col. 2, lines 1-7).

However Perrig does not discloses the method wherein verifying the HMAC value with the other hash key comprising, computing a (H) associated with a hash message authentication code for a given H=HMAC, where F*i* corresponds to the data being signed, S the key for signing, an comparing the computed value with the retrieved HMAC value from the frame.

Carro discloses the method wherein verifying the HMAC value with the other hash key comprising, computing a (H) associated with a hash message authentication code for a given H=HMAC (para 0027, lines 1-5; para 0032 lines 1-24; para. 0028, lines 4-8), when F corresponds to the data being signed, S the key for signing, an comparing the computed value with the retrieved HMAC value from the frame (para. 0032, lines 16-20). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Perrig to include the use of decrypting an HMAC frame such that the received frame may be compared with the previous frames in order to determine if the received HMAC value is valid or not.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esteve Mede whose telephone number is 571-270-1594. The examiner can normally be reached on Monday thru Friday, 8:30-5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Esteve Mede

EM

October 3, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER